Office of Information Security Newsletter

July 2006
Volume 1 Issue 4

Inside This Issue

1 Prevent Data Theft

2 Wireless Access

Security by Wandering Around
(SBWA) is a way for all of us to participate in protecting State assets. At lunch time, or on a break, wander around your work area and look for security concerns - such as a desktop/laptop that is logged on but unattended, or a monitor positioned so that it allows sensitive information to be seen by visitors. You can print the coupons from the link below and leave them as reminders for co-workers to keep state information secure. SBWA Coupons

PREVENT DATA THEFT

If you've been traveling for a while, you've probably experienced the nightmare of boarding your plane without a key piece of luggage. If that piece is your laptop, you might be considering that dream flight to Hawaii rather than explain the loss of your laptop! Your mind races; "have I just placed the state and its citizen's confidential data directly into the hands of a criminal?"

As workers become more and more mobile, and as the computing we all depend on becomes more powerful, increasing volumes of data are floating around, largely unprotected, on laptops! As that laptop travels well beyond the bounds of the office, this data becomes much less secure. Without adequately protecting the data on board your mobile computer, you are virtually inviting a criminal inside the state's networks.

Notice some recent headlines:

Computerworld.com reports, June 7, 2006**,** The American Institute of Certified Public Accountants (AICPA) today confirmed that a computer hard drive containing the unencrypted names, addresses and Social Security numbers of nearly all of its 330,000 members has been missing since February.

Computerworld.com reports; Red Cross warns 1 million blood donors in Missouri and Illinois that their personal data could have been stolen earlier this year.

An Associated Press article on HeraldTribune.com reports; Personal data of up to 50,000 active Navy and National Guard personnel were among those stolen from a Department of Veterans Affairs (VA) employee last month.

The Providence Journal reports, the YMCA is the latest organization to disclose a computer theft that puts people at risk of identity fraud.

What can we do to help protect the state's confidential data?

- Conduct a risk analysis and look at the kind of information that is stored on the agencies network, and who has access to it.
- Control access to the data.
- Compartmentalize people's access to data on a need to know basis. Does everyone need full access to the customer database or accounts? Can you give people more limited access? For example, by using an access-controlled database rather than a spreadsheet?

Wireless Access

- Perform a thorough site survey. Make sure your wireless coverage is adequate for employees, but not your neighbors.
- Be courteous - ensure that your wireless access is not interfering with others.
- Do **NOT** use WEP encryption as it is easily compromised. Secure all wireless access points in accordance with 802.11 – wireless standard.
- Scan for unauthorized wireless access points often.

Defending Nevada's Technology

State of Nevada
Office of Information Security - DoIT
1340 S. Curry Street
Carson City, NV 89703
Phone (775) 684-5800
Fax (775) 687-1155
Email: infosec@state.nv.us
Website: http://infosec.nv.gov

PREVENT DATA THEFT (Cont.)

- Have clear policies about what employees can do with confidential or agency-critical data. Educate the workforce.
- Encrypt confidential data.
- Educate users about the importance of passwords and ensure that employees use strong passwords. They should be treated like office keys and not shared or compromised in any way.
- Educate users about the risks of social engineering.(see April '06 OIS newsletter)
- Delete users' access privileges once they stop working for the agency.
- When disposing of old equipment, ensure that it is securely cleared of any information including passwords.

Although the cost of losing the laptop hardware itself can be very high (the cost of the laptop itself and any equipment can be many thousands of dollars), the loss of software and data on the laptop and the potential embarrassment, exposure, and liability that result from the loss of confidential state and client data can be far more expensive.

As state employees' let us all do our part to ensure the safety of the confidential data that has been entrusted to us.

WIRELESS ACCESS

On the surface, installing wireless seems to be a great choice. There are no costs of 'regular' wiring, and the computer users have freedom in placing their computers where they want in the offices. There's no downside, right? Unfortunately, the harmful consequences of wireless are oftentimes overlooked until it is too late.

A **properly planned and secured** wireless solution can be achieved, and is a reasonable solution in specific cases. However, there are many factors that need to be taken into account before an agency starts the wireless access process. A few of the more important issues are:

- Have you received approval to have wireless on your network? This may be a management issue, but often crosses boundaries to others when traversing the SilverNet backbone.
- Will you be able to provide stable wireless access to all of your legitimate users, without broadcasting your data outside your office or building? A properly performed site survey will assist you in planning the coverage.
- Are your wireless access points going to be interfering with other businesses or agencies wireless access in a shared office building?
- Secure **all** wireless access points in accordance with 802.11 – wireless standard.
- Run frequent wireless assessment scans to detect rogue access points in the network. It only takes a single unsecured access point to allow an intruder access into your internal network. Often, these are installed by employees in an attempt to be helpful, not realizing the vulnerability that they are exposing to the internal network.
- How critical is access to the network for the wireless employees? Wireless signals are susceptible to interference (accidental or intentional) that can disrupt service.

You may notice that only one of these directly addresses security. While the security of the wireless access is vital, it is only one of many considerations an agency should take into account before taking the plunge into the wireless world.